MEDIDAS DE VIGILÂNCIA EM DISPOSITIVOS MÓVEIS COMO FORMA DE VIOLAÇÃO DA PRIVACIDADE E PROTEÇÃO DE DADOS

Guilherme Guolo Brígido[1],Rogério Antônio Casagrande[2]

Resumo: Vigilância e violação de privacidade são temas recorrentes após o advento dos meios tecnológicos de comunicação e, além disso, a segurança desses meios necessita de certa atenção. A presente pesquisa visa evidenciar estes temas e buscar medidas de proteção no intuito de minimizar os riscos relacionados à vigilância, violação de privacidade e a segurança de usuários, prioritariamente de dispositivos móveis. A pesquisa tem como objetivo criar um conjunto de medidas de proteção a serem utilizadas por usuários com pouco ou nenhum conhecimento prévio em relação a segurança de dados. A aquisição dos dados foi realizada através de bases de dados científicos, buscando artigos que trouxessem informações a respeito de medidas de proteção e segurança, além de analisar seus resultados e exemplificar o funcionamento das medidas selecionadas. O conjunto de medidas gerado como resultado final pode proporcionar aos usuários um maior nível de segurança caso seja posto em prática, porém conclui-se que, ao trazer mais segurança aos usuários, o uso de certas medidas de proteção pode se tornar inconveniente.

Palavras-chave: Vigilância. Violação de Privacidade. Segurança de Dados. Medidas de Proteção.

[1] Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) Criciúma – SC – Brasil. guilhermeguolobrigido@gmail.com

[2] Curso de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) Criciúma – SC – Brasil. roc@unesc.net

ABSTRACT: Surveillance and violation of privacy are recurring themes after the advent of technological means of communication and, in addition, the security of these means needs some attention. The present research aims to highlight these themes and seek protective measures in order to minimize the risks related to surveillance, violation of privacy and user safety, primarily from mobile devices. The research aims to create a set of protection measures to be used by users with little or no prior knowledge regarding data security. Data acquisition was carried out through scientific databases, seeking articles that brought information about protection and safety measures, in addition to analyzing their results and exemplifying the operation of the selected measures. The set of measures generated as a final result can provide users with a higher level of security if put into practice, but it is concluded that, by bringing more security to users, the use of certain protection measures can become inconvenient.

Keywords: Surveillance. Violation of Privacy. Data Security. Protection Measures.

1 INTRODUÇÃO

Os meios de comunicação móveis, mais populares na figura dos smartphones de última geração, vieram para facilitar a vida dos usuários de maneira geral. Porém, apesar de todas as melhorias e facilidades que isso possa trazer, podem ocorrer situações de uso indevido das informações pessoais de usuários e, em casos mais específicos, vigilância quase que total sobre estes usuários.

A real possibilidade de monitoramento das pessoas pelo Estado e por empresas, por meio da Internet, ensejou a retomada das discussões sobre o que a privacidade significa em um mundo em que as pessoas fornecem voluntariamente uma quantidade muito grande de dados pessoais, não mais apenas pelos meios tradicionais de preenchimento de cadastros, mas pelo rastreamento dos seus relacionamentos interpessoais, pensamentos e interesses (TOMASEVICIUS FILHO, 2014).

Segundo Lyon (2017, tradução nossa), a partir do século XX, os meios corporativos e estatais, inclinaram-se para a vida cotidiana por meio de infraestruturas de informação e também da crescente dependência de tecnologias digitais nas relações pessoais. Tratando-se de dependência de tecnologias digitais, os

dispositivos móveis são os mais utilizados pelo grande público, especialmente smartphones de todos os modelos existentes.

De acordo com Wolfe (2017, tradução nossa), o risco de ser monitorado sempre existirá e que, como a imensa maioria das pessoas não poderia ficar sem os seus smartphones, deveriam se atentar sobre como sua privacidade pode ser comprometida por diversos meios e também sobre medidas de proteção contra vigilância indesejada. Na maioria dos casos, a decisão de se arriscar ser alvo de vigilância parte da conveniência dos usuários em utilizar os serviços prestados ou simplesmente não pensarem a respeito e, no caso de aceitarem utilizar determinados serviços, verificar os benefícios e o esforço, tempo e recursos necessários para mitigar os riscos subsequentes.

Em muitos países foram criados marcos regulatórios com o objetivo de proteger dados pessoais dos cidadãos, inclusive no Brasil, com a lei geral de proteção de dados (LGPD) (BRASIL, 2018). Esses marcos regulatórios reconhecem os dados pessoais como elementos juridicamente relevantes, estabelecendo direitos e limites às empresas prestadoras de serviços, organizações e plataformas de dados (BIONI et al., 2020). Além disso, se impõe limites ao uso lícito de dados adquiridos dos usuários. Algo perceptível é a preocupação jurídica que se tem a respeito do tema, principalmente partindo da Europa e consequentemente para o resto do mundo.

Partindo do pressuposto de haver a possibilidade de pessoas serem vigiadas e, em muitos casos, terem sua privacidade violada, poderia ser importante a existência de medidas de proteção e estudo da efetividade das mesmas para o benefício de usuários comuns.

O crescimento na utilização dos smartphones trouxe também preocupações relativas ao uso não autorizado da informação fornecida pelos usuários (NETTO; SILVA; MAÇADA, 2018)

Mesmo sem a utilização do GPS ou de conexão com a Internet, ainda existem maneiras de se localizar um dispositivo. Serviços de localização da Google fornecem aplicativos com a localização do dispositivo sem o uso de GPS. Aplicações nocivas podem utilizar dados de localização para encontrar usuários (BIONE, 2015).

Nesta pesquisa, com o objetivo de elucidar e trazer medidas e tecnologias a serem utilizadas por usuários comuns contra a violação de privacidade, vigilância e propor métodos mais seguros em relação a ataques, foram analisadas possibilidades e elaborado um conjunto de medidas de defesa, avaliando casos onde há a

possibilidade de um usuário comum utilizar, como por exemplo tecnologias e ações do próprio usuário.

2 TRABALHOS CORRELATOS

Diversos trabalhos sobre vigilância em dispositivos móveis foram publicados em diversos periódicos, como por exemplo, os publicados na revista IEEE Xplore. A pesquisa realizada por Wolfe (2017, tradução nossa), demonstra como os smartphones podem ser utilizados como ferramentas de vigilância utilizando tecnologias como GPS, RFID, Wi-Fi, Bluetooth e muitos outros sensores que compõem estes aparelhos. O objetivo do artigo é demonstrar como smartphones são utilizados como ferramenta de vigilância e rastreamento, incluindo aplicações abusivas e dos riscos de seu uso de como os usuários podem se proteger do monitoramento indesejado.

Sendo este o objetivo, são listadas formas de vigilância e alguns meios de proteção. A pesquisa enfatiza a ação por parte de governos e suas agências de inteligência em todo o mundo para vigiar indivíduos e organizações, se utilizando de métodos variados como interceptações de canais de comunicação, sensores, câmeras e também malwares. Para cada tecnologia e técnica citada no artigo, o autor a descreve como funcionam e também seus riscos para a segurança de um dispositivo móvel.

O artigo demonstra que nenhum método de proteção é totalmente eficaz, porém muitos deles são importantes para mitigar os danos de uma possível invasão ou vigilância indesejadas. O autor cita que muitos usuários acabam por não utilizar medidas de segurança por desconhecimento ou conveniência, porém, esclarece que cabe a cada usuário tomar a decisão de aplicar, ou não, medidas de proteção contra vigilância.

Malinka et al. (2022, tradução nossa), apresenta um estudo direcionado às exigências da *Payment Services Directive 2* (PSD2) em vigor na União Europeia. Os autores trazem um panorama geral dos métodos de autenticação utilizados na segurança do e-banking, sua conformidade com os padrões modernos e sua resistência quanto a ataques. Para apresentar a visão geral, os autores introduziram a taxonomia dos métodos de ataques ao e-banking de acordo com as ameaças do autenticador das Diretrizes de Identidade Digital do *National Institute of Standards and*

*Technology (*NIST). O objetivo dos autores foi de trazer uma visão abrangente em relação aos métodos de autenticação e suas avaliações de segurança, abordando dispositivos e fontes variados.

Blaise, Awodele e Yewande (2021, tradução nossa) tratam do problema da vigilância em dispositivos móveis e tem como foco o estudo de algoritmos criptográficos, como o Data Encryption Standard (DES) para uma possível solução deste problema.

A metodologia utilizada propõe analisar a performance de vários algoritmos criptográficos. A metodologia foi dividida em três partes principais, sendo: parâmetros da simulação, parâmetros de validação de performance e implementação da simulação. Os parâmetros da simulação podem ser divididos entre a fase de entrada dos dados, a fase de criptografia e descriptografia e a fase de visualização dos resultados. Na validação de performance são analisados tempo de criptografia, tamanho de chave diferente, utilização de CPU, taxa de consumo de memória e tempo de processo geral. A implementação trata dos tipos de dados de entrada, tamanhos, demonstra o hardware e softwares utilizados na implementação dos algoritmos escolhidos, sendo as entradas sempre as mesmas para que não ocorram problemas na análise dos resultados.

Ao final do artigo, os autores fazem a comparação dos algoritmos de criptografia tendo como base os parâmetros metodológicos citados e demonstra estes dados através de gráficos. Analisando os resultados, se chegou à conclusão de que o algoritmo de criptografia híbrido seria o mais seguro a se utilizar e manter a confidencialidade dos dados e, ao ser aplicado em um cenário de criptografia de ponta-a-ponta, aumentaria sua efetividade e segurança.

Ghasemi et al. (2015, tradução nossa), propõem a criação de um sistema para monitoramento de fluxo de informação e reconhecimento de contexto utilizando redes bayesianas, juntamente com o auxílio da tecnologia *TaintDroid*, utilizada para prevenção de vazamento de dados pessoais de aplicativos instalados.

O estudo enfatiza a dificuldade encontrada em realizar o rastreamento de informações em sistemas operacionais leves, como iOS, ao contrário de sistema operacionais pesados, como Windows e Linux. O sistema proposto utilizaria a técnica de rastreamento de fluxo de informações e contaminação de dados para rastrear informações confidenciais do usuário e controlar seus vazamentos e realiza a tentativa

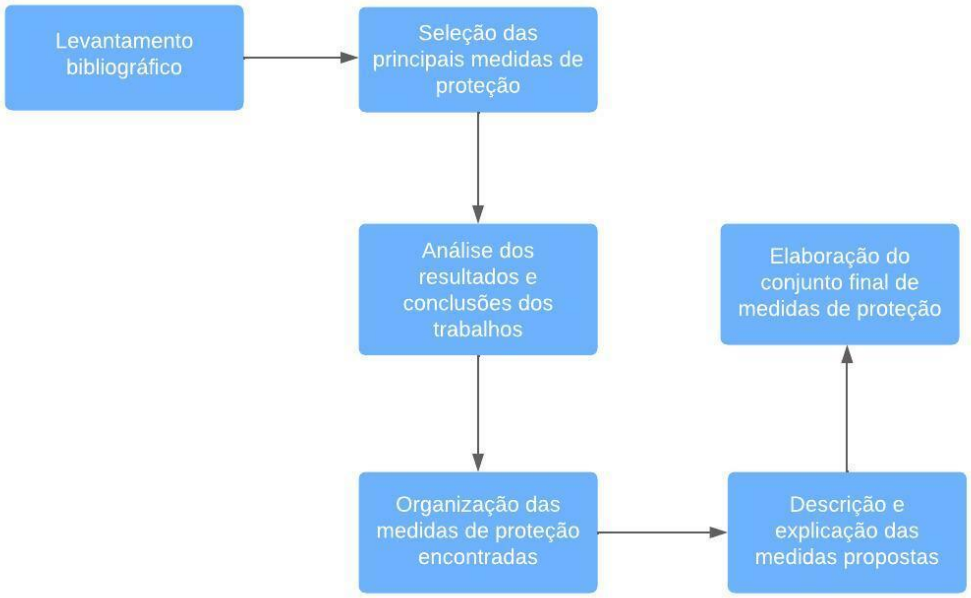
de extrair o tipo e a força de uma relação entre usuários para controlar informações compartilhadas entre eles.

Como conclusão do estudo, os autores descobriram que o sistema proposto teria algumas limitações em relação à sua aplicação. Um dos problemas seria ó fato de que o sistema não é compatível com qualquer smartphone Android. Concluíram, também, que categorizar os usuários com base em seu tipo de conexão acabou por não ser um método muito refinado.

3 MATERIAIS E MÉTODOS

A partir desta pesquisa, que é de categoria exploratória, com base tecnológica e descritiva, foram realizados buscas e estudos em bases de dados e trabalhos científicos, como os encontrados na revista IEEE Xplore para obtenção de medidas de proteção contra vigilância e violação de privacidade em dispositivos móveis e demais dispositivos eletrônicos. Ela objetivou a criação de um conjunto de medidas de segurança possíveis de ser utilizadas por usuários comuns, ou seja, pessoas com pouco ou nenhum conhecimento referente a área de segurança de dados. A figura 1 demonstra as etapas de desenvolvimento da pesquisa, que envolve o levantamento bibliográfico, seleção das medidas de proteção até a elaboração final do conjunto de medidas.

Figura 1 Fluxograma das etapas de desenvolvimento



Fonte: Do autor (2022).

3.1 AQUISIÇÃO DOS ARTIGOS E TRABALHOS CIENTÍFICOS

Os artigos e trabalhos científicos foram adquiridos através da base de dados da IEEE Xplore, que é a plataforma agregadora de trabalhos científicos da IEEE, acessada via plataforma de periódicos Capes, artigos de universidades brasileiras como a USP (Universidade de São Paulo). O armazenamento dos artigos foi realizado utilizando a ferramenta Mendeley, de onde foi possível realizar a leitura e referencia-los na pesquisa. Primeiramente foi realizado o levantamento bibliográfico dos trabalhos na área de segurança de dados, para que fosse realizada a análise de temas e resultados em busca de exemplos de medidas de proteção contra vigilância e violação de privacidade. A busca pelos trabalhos científicos foi realizada dando prioridade a medidas possíveis de serem aplicadas em dispositivos móveis e que dependesse, o menos possível, de conhecimento prévio por parte de usuários comuns.

3.2 SELEÇÃO DAS MEDIDAS DE PROTEÇÃO

Após a aquisição dos trabalhos e dados científicos, foram selecionadas quatro principais medidas recomendas: Autenticação multifator, VPN (*Virtual Private Network*), gerenciadores de senhas e o uso dos padrões WPA para redes Wi-Fi, prioritariamente o WPA3. Selecionadas as principais medidas de proteção, estas foram exemplificadas e seus mecanismos de proteção analisados através dos resultados das pesquisas encontradas. Os critérios utilizados para a escolha das medidas foram: capacidade de anonimizar o usuário nas redes, capacidade de proteger credenciais de acesso, capacidade de evitar ataques de determinadas fontes e as dificuldades que um usuário comum poderia ter para utilizar determinada medida. Estes pontos foram obtidos através do estudo do funcionamento de cada uma das medidas escolhidas, assim como os tipos de criptografias utilizadas, análise de fatores de autenticação e, através disso, verificar a possibilidade de determinada medida cumprir com seu objetivo, tanto em segurança propriamente dita, como de anonimato.

3.3 ELABORAÇÃO DO CONJUNTO DE MEDIDAS DE PROTEÇÃO

Após a seleção, o estudo e análise das medidas de proteção, o conjunto de medidas foi elaborado na forma de lista, com explicações de detalhes em relação ao funcionamento, tecnologias adotadas e trazendo justificativas de se usar cada medida contida no conjunto.

Adicionalmente, medidas recomendadas, porém consideradas mais simples, com menor possibilidade de uso por parte de usuários comuns ou que seu uso possui um risco considerável por parte de usuários com pouco conhecimento tecnológico. Referente às medidas simples, estão ações que podem ser tomadas sem que o usuário se utilize de tecnologias externas ou métodos e, a respeito de medidas que possuem riscos, está o exemplo da criptografia de disco. Estes dados foram colocados em uma tabela separada das medidas principais, considerando se é uma tecnologia ou ação, se possui risco por parte do usuário e se possui a necessidade de conhecimento prévio para ser utilizado.

4 RESULTADOS E DISCUSSÃO

Dados acerca dos métodos e tecnologias a serem utilizadas para proteção contra vigilância e violação de privacidade puderam ser observados através de pesquisa em artigos e trabalhos científicos publicados na área de segurança da informação, sendo assim, chegou-se a um conjunto de medidas principais a serem consideradas, juntamente com recomendações adicionais recomendadas a usuários comuns.

A pesquisa realiza por Malinka et al. (2022), além de citar métodos de autenticação recomendados pelo *National Institute of Standards and Technology (*NIST), mostra que uma combinação de fatores diferentes de autenticação resulta em um nível maior de segurança, desde que haja independência dos fatores, ou seja, caso um dos fatores seja violado, não comprometa a integridade dos demais. Um exemplo deste tipo de comprometimento são casos onde outros fatores de autenticação estão presentes no mesmo local, como por exemplo a autenticação via e-mail e SMS (*Short Message Service*) serem utilizadas no mesmo dispositivo. Em casos de roubo do Smartphone, o invasor teria total condição de acesso às informações no próprio aparelho e, se tratando de sistemas bancários instalados no aparelho, o prejuízo de uma autenticação comprometida pode ser crítico. A figura 1 abaixo demonstra os fatores primitivos de autenticação combinados, ou não, avaliando pontos como proteção contra clonagem de memória, independência do fator e força da senha, conforme a Diretiva de Serviços de Pagamento (PSD2) europeia.

Tabela 1 - Métodos de autenticação

Combinação de métodos	**Proteção contra clonagem**	**Independência do fator**	**Autenticação forte**
Senha	Não	Não	Não
Senha + PIN	Não	Não	Não
Token de hardware protegido por PIN	Sim	Sim	Sim
Token de hardware protegido por biometria	Sim	Sim	Sim
SMS	Sim	Não	Não
Senha + SMS	Sim	Sim	Sim

Senha dinâmica + biometria	Não	Sim	Sim
Biometria	Não	Não	Não
Biometria + senha	Não	Sim	Sim
Biometria + SMS	Sim	Sim	Sim
Secure enclave protegido por biometria	Sim	Sim	Sim
Secure enclave protegido por senha	Sim	Sim	Sim

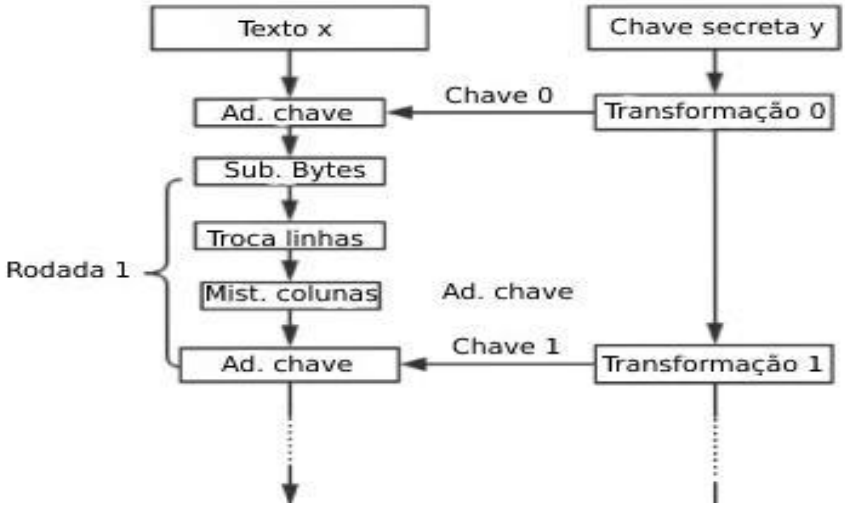
Fonte: Adaptado de Malinka et al. (2022).

Como é possível observar, alguns fatores, quando utilizados isoladamente, não fornecem grande proteção, como é o caso do uso da senha. Porém, ao serem combinados com outros fatores, pode-se adquirir uma maior segurança. É importante analisar que, utilizando como exemplo a combinação de senha e SMS, que o aparelho receptor do SMS não deve ser o mesmo aparelho em que a senha é colocada, pois isso comprometeria a segurança da autenticação. Existem alguns cuidados a serem tomados para manter as credenciais seguras, como por exemplo tomar cuidados em relação a sites falsos e links não confiáveis, pois desta forma há o risco de o usuário ser vítima de *phishing scam*, sendo este um método comum de engenharia social para obtenção de dados dos usuários. O uso de autenticação multifator possui a capacidade de melhorar a segurança de dados de acesso aos dispositivos e plataformas utilizadas pelos usuários, porém o uso dessa medida pode se tornar inconveniente em certos casos.

Para casos em que a vigilância ou censura são proeminentes, o uso de VPN permite burlar bloqueios de acesso e consegue ocultar a atividade online dos provedores de internet, pois os dados não trafegam abertamente e o IP fica restrito à conexão criptografada. Porém, ao se conectar em uma VPN, os dados digitados ou acessados, estarão visíveis ao provedor da VPN, desta forma é recomendável que seja realizada uma análise prévia da idoneidade do serviço utilizado. O estudo realizado por Jayatilleke e Pathirana (2018), relata o caso em que as mídias sociais foram banidas do Sri Lanka, onde por volta de 85% dos usuários questionados utilizaram redes VPN burlar este bloqueio. Uma VPN evita coleta de dados online bloqueando o acesso à conexão do usuário, porém é recomendado que sejam

utilizadas aplicações VPN conhecidas e confiáveis, no intuito de minimizar os riscos de vazamento de dados. Quando todos os bits de tráfego da Internet que saem e chegam ao dispositivo do usuário são criptografados, este se torna anônimo. Uma VPN considerada como segura normalmente não é gratuita e, muitas das vezes, utiliza criptografia AES (*Advanced Escryption Standard*) de 256 bits, sendo o padrão de criptografia AES de 256 bits resistente a ataques devido a quantidade de rodadas utilizadas no processo de criptografia e dos recursos necessários para a quebra de sua chave criptográfica. A figura 2 demonstra os passos realizados pela criptografia AES de 256 bits.

Figura 2 Passos da criptografia AES-256



Fonte: Adaptado de Su ,Zhang e Li (2019).

Como é possível analisar, a estrutura interna do algoritmo AES consiste em quatro etapas básicas, sendo a substituição de bytes, troca de linhas, mistura de colunas e adição da chave de rodada. Este processo é realizado sucessivamente até a décima rodada, tendo como resultado o texto final criptografado.

Para proteção e criptografia de senhas para aplicativos instalados e acesso a sites através de senhas e demais credenciais, é possível o uso de gerenciadores de senha. Gerenciadores de senha permitem gravar senhas e demais credenciais em um “cofre” protegido por uma senha mestra. Conforme estudo realizado por Yu e Yin (2021), analisando os gerenciadores de senhas 1Password, LastPass e Keepass, sendo este último não compatível com sistema operacional Android ou IOS. Os gerenciadores testados utilizando algoritmo KDF (*Key Derivation Function*), utilizando

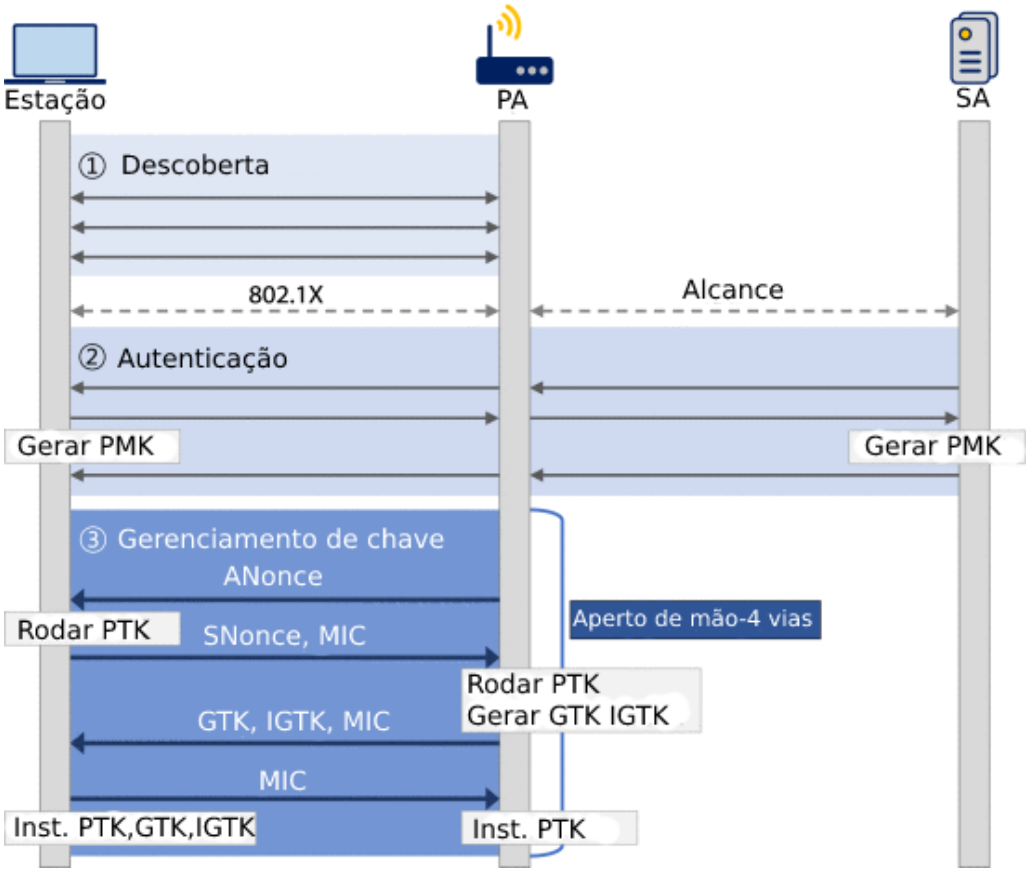
um grande número de iteração, variando entre um gerenciador e outro. Os gerenciadores foram testados utilizando método de força bruta, testando milhares de senhas em cada rodada.

A segurança de um bom gerenciador de senhas depende, em parte, de uma senha mestra longa e diversificada, ou seja, uma senha forte. Além disso, uma grande quantidade de iterações é desejável para aumentar a segurança do gerenciador. É recomendável que a senha mestra para acesso ao gerenciador de senhas não seja armazenada dentro do mesmo, pois isso poderia comprometer a segurança ao cofre e, consequentemente, a segurança de todas as credenciais guardadas. Uma maneira de proteger as credenciais, é permitir que o gerenciador gere uma senha segura e, para acesso aos aplicativos e sites, o usuário seja obrigado a digitar um texto complementar para a credencial. Desta forma, mesmo que o cofre seja comprometido, o invasor não terá acesso direto à totalidade das credenciais.

Em relação a redes Wi-Fi, é recomendável que os usuários não se conectem em redes públicas, sendo preferível a conexão apenas em redes protegidas pelos padrões WPA (*Wi-Fi Protected Acces*), pois este utiliza de criptografia proteger as mensagens enviadas. A partir de 2018 o padrão WPA foi atualizado para sua terceira versão, sendo o WPA3, porém o WPA2 ainda é mais comum. Utilizar desses cuidados é importante para que o usuário não fique vulnerável à ataques como o *Man-in-the-Middle*, que intercepta o tráfego na rede e consegue acesso a informações importantes dos usuários.

A figura 3 ilustra as três fases do WPA2, sendo as fases de descoberta, autenticação e gerenciamento de chave. A primeira fase, a fase de descoberta, possui três trocas de mensagens, a estação se associa com o ponto de acesso (PA) para troca de cifras. Na segunda fase, a fase de autenticação, serão geradas através da chave mestra (MK), os pares de chave mestra (PMK). Na terceira fase, ambas as partes derivam a chave temporal par a par (PTK) e confirmam a posse do mesmo PTK usando o aperto de mão em quatro vias. O PTK é novo em cada associação, pois é derivado dos pares de chave mestra (PMK) e de dois números aleatórios (ANounce e SNonce), respectivamente, escolhidos por cada parte para uma única associação.

Figura 3 Três fases do WPA2



Fonte: Adaptado de Kwon e Choi (2021, tradução nossa).

Algumas recomendações aos usuários, serão listadas de forma mais simplificada, pelos seguintes motivos: requerem conhecimento tecnológico prévio para uso e configuração por parte de usuários comuns, impossibilidade de uso em determinados aparelhos ou simplesmente por serem ações a serem tomadas pelos usuários no dia a dia.

A tabela 2 ilustra medidas secundárias recomendadas aos usuários, evidenciando se a medida seria uma ação tomada parte do usuário ou tecnologia a ser utilizada, como é o caso da criptografia de disco. Para proteger dados de discos rígidos e cartões de memória, é possível utilizar a criptografia de disco. Esse é um método disponível em dispositivos móveis e possibilita que o usuário criptografe os dispositivos de armazenamento e proteja-os com senha, impedindo que agentes externos tenham acesso aos dados originais. Situações comuns como perda ou roubo do dispositivo de armazenamento podem colocar em risco informações importantes do usuário e comprometer a segurança dos dados. O uso desse tipo de recurso possui alguns pontos negativos, sendo o mais importante deles o risco de, ao criptografar os

dados no aparelho celular ou unidade de armazenamento, o usuário acabar esquecendo a senha para decriptar os dados, o que acarreta na perda dos dados.

O aplicativo *SnoopSnitch*, listado na tabela 2, pode ser utilizado para analisar o smartphone do usuário e descobrir falhas de segurança, como por exemplo casos onde o usuário está sendo vítima dos chamados coletores IMSI, que interceptam informações do aparelho. Este aplicativo possui limitações em relação a sua utilização, pois depende que o aparelho esteja em *root,* requer que o aparelho possua um chip Qualcomm para funcionar integralmente e suas configurações requerem um conhecimento relativamente elevado.

Tabela 2 Medidas secundárias recomendadas

Medida	**Conhecimento prévio**	**Risco por parte do usuário**	**Tipo**
Criptografia de disco	Sim	Alto	Tecnologia
Desativar o *Tracking* do Google Maps	Não	Baixo	Ação do usuário
Não instalar aplicativos de fontes desconhecidas	Não	Baixo	Ação do usuário
Não dar permissões a Apps além do necessário para funcionamento do mesmo	Não	Baixo	Ação do usuário
Não inserir dados pessoais em redes sociais e sites desconhecidos	Não	Baixo	Ação do usuário
Evitar inserir credenciais em computadores ou dispositivos de terceiros	Não	Baixo	Ação do usuário
Utilizar senhas fortes, com caracteres diversificados	Não	Baixo	Ação do usuário
Não acessar endereços desconhecidos diretamente via QR Code	Não	Baixo	Ação do usuário
Aplicativo SnoopSnitch	Sim	Alto	Tecnologia

Fonte: Dados da pesquisa (2022).

5 CONCLUSÃO

Nesta pesquisa, foram buscadas as principais medidas de proteção contra vigilância e violação de privacidade em bases de dados e trabalhos científicos de modo a criar um conjunto de medidas que possam ajudar a preservar a privacidade e manter a segurança dos dados dos usuários e, ao mesmo tempo, possíveis de serem utilizadas por pessoas sem muito conhecimento prévio em relação a segurança de dados.

O conjunto gerado como resultado da pesquisa possui medidas que variam de ações simples por parte do usuário a tecnologias a serem utilizadas pelos mesmos. Através da análise das tecnologias listadas e pesquisas científicas pesquisadas, conclui-se que muitos dos usuários de tecnologias móveis e demais plataformas, utilizam pouca ou nenhuma medida para se proteger em casos de violação de privacidade e vigilância. Muitas dessas medidas recomendadas no conjunto final, podem aumentar trazer um aumento da segurança dos usuários em relação a proteção de credenciais, anonimato na internet e também segurança em redes sem fio. Porém, em contrapartida aos benefícios de se proteger, boa parte destas mesmas medidas pode tornar os processos de segurança, acesso e autenticação mais demorados e menos práticos aos usuários. Sendo assim, para muitos dos usuários, a segurança adquirida pode não compensar a morosidade do processo.

A área de segurança de dados se mostrou muito abrangente e complexa, desta forma a pesquisa enfatizou alguns pontos mais relevantes e de fácil acesso. Por motivos de não haver tempo hábil para tal, não houve a implementação de algoritmos ou métodos computacionais listados.

Para trabalhos futuros, sugere-se a implementação de testes práticos ou simulações de ataques para uma ou mais medidas listadas, como por exemplo um gerenciador de senhas, no intuito de se avaliar dados mais precisos em relação ao nível de segurança adquirido com o uso do mesmo.

REFERÊNCIAS

BIONE, T. A. MITIGAÇÃO DE RISCOS DE SEGURANÇA DE DISPOSITIVOS ANDROID BASEADA NA MELHORIA DAS DECISÕES DE CONFIGURAÇÃO DO USUÁRIO. **UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO**, 2015.

BIONI, B. et al. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Grupo Editora Nacional, 2020.

BLAISE, O. O.; AWODELE, O.; YEWANDE, O. An Understanding and Perspectives of End-To-End Encryption. **International Research Journal of Engineering and Technology (IRJET)**, n. April, 2021.

BRASIL. **L13709**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 nov. 2021.

GHASEMI, H. et al. **Pervasive privacy: A practical context-aware system to preserve privacy on android smartphones**. 2015 7th Conference on Information and Knowledge Technology, IKT 2015. **Anais**...Institute of Electrical and Electronics Engineers Inc., 2 out. 2015

JAYATILLEKE, A.; PATHIRANA, P. Smartphone VPN App Usage and User Awareness among Facebook Users. **2018 National Information Technology Conference, NITC 2018**, 27 nov. 2018.

KWON, S.; CHOI, H. K. Evolution of Wi-Fi Protected Access: Security Challenges. **IEEE Consumer Electronics Magazine**, v. 10, n. 1, p. 74–81, 1 jan. 2021.

LYON, D. Surveillance culture: Engagement, exposure, and ethics in digital modernity. **International Journal of Communication**, v. 11, p. 824–842, 2017.

MALINKA, K. et al. E-Banking Security Study-10 Years Later. **IEEE Access**, v. 10, p. 16681–16699, 2022.

NETTO, Y. W. C.; SILVA, V. R. R. B. DA; MAÇADA, A. C. G. Desenvolvimento e Validação de um Instrumento para Mensurar a Preocupação de Usuários de Smartphones sobre a Invasão de Privacidade. **Revista Gestão & Tecnologia**, v. 18, n. 3, p. 73–96, 21 ago. 2018.

SU, N.; ZHANG, Y.; LI, M. Research on data encryption standard based on AES algorithm in internet of things environment. **Proceedings of 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2019**, p. 2071–2075, 1 mar. 2019.

TOMASEVICIUS FILHO, E. Em direção a um novo 1984? A tutela da vida privada entre a invasão de privacidade e a privacidade renunciada. **Revista da Faculdade de Direito, Universidade de São Paulo**, v. 109, p. 129, 2014.

WOLFE, H. B. **The Mobile Phone as Surveillance Device: Progress, Perils, and Protective MeasuresIEE Computer Society**IEEE Computer Society, , 1 nov. 2017.

YU, F.; YIN, H. **A Security Analysis of the Authentication Mechanism of Password Managers**. International Conference on Communication Technology Proceedings, ICCT. **Anais**...Institute of Electrical and Electronics Engineers Inc., 2021